AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of preventing an attack on a network, the method comprising the computer-implemented steps of:

receiving an ICMP packet, wherein ~~a data field within~~ the ICMP packet ~~includes~~ carries a portion of a header associated with a connection in a connection-oriented transport protocol, and wherein the portion of the header includes a packet sequence value associated with the connection;

obtaining the packet sequence value from the portion of the header that is ~~included within the data field~~ carried within the ICMP packet;

authenticating the ICMP packet by determining if the packet sequence value from the portion of the header that is ~~included within the data field~~ carried within the ICMP packet is valid; and

responding to the ICMP packet by updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid.

2. (Currently Amended) A method as recited in Claim 1, ~~wherein the step of receiving an ICMP packet comprises receiving an ICMP packet, wherein the data field within~~ the ICMP packet ~~includes~~ carries a portion of a TCP header associated with a TCP connection.

3. (Original) A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP "endpoint unreachable" error packet.

4. (Original) A method as recited in Claim 1, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed.

5. (Previously Presented) A method as recited in Claim 1, wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection.

6. (Previously Presented) A method as recited in Claim 1, wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of sent but unacknowledged TCP packet sequence values for the connection.

7. (Previously Presented) A method as recited in Claim 1, wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is exactly equal to one or more sequence values of one or more packets that are then-currently stored in a TCP re-transmission buffer, starting at a sequence value of a previously sent segment that resulted in receiving the ICMP packet.

8. (Original) A method as recited in Claim 1, wherein the steps are performed in a router acting as a TCP endpoint node.

9. (Original) A method as recited in Claim 1, wherein the steps are performed in a firewall device.

10. (Currently Amended) A method of preventing an attack on a network, the method comprising the computer-implemented steps of:

receiving, at a TCP endpoint node in a TCP/IP packet-switched network, an ICMP packet, wherein ~~a data field within~~ the ICMP packet ~~includes~~ carries a portion of a TCP header associated with a TCP connection;

obtaining a packet sequence number from the portion of the TCP header that is ~~included within the data field~~ carried within the ICMP packet;

authenticating the ICMP packet by determining if the packet sequence number from the portion of the TCP header that is ~~included within the data field~~ carried within the ICMP packet is valid; and

responding to the ICMP packet by updating a maximum transmission unit (MTU) value associated with the TCP connection only if the packet sequence number is determined to be valid.

11. (Original) A method as recited in Claim 10, wherein the step of receiving an ICMP packet comprises receiving an ICMP "endpoint unreachable" error packet.

12. (Original) A method as recited in Claim 10, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed.

13. (Previously Presented) A method as recited in Claim 10, wherein the step of authenticating the ICMP packet by determining if the packet sequence number is valid comprises determining if the packet sequence number is within a range of TCP packet sequence numbers that are allowed for the connection.

14. (Previously Presented) A method as recited in Claim 10, wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence number is within a range of sent but unacknowledged TCP packet sequence values for the connection.

15. (Previously Presented) A method as recited in Claim 10, wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence number is equal to one or more sequence numbers of one or more packets that are then-currently stored in a TCP re-transmission buffer, starting at a sequence value of a previously sent segment that resulted in receiving the ICMP packet.

16. (Original) A method as recited in Claim 10, wherein the steps are performed in a router acting as a TCP endpoint node.

17. (Original) A method as recited in Claim 10, wherein the steps are performed in a firewall device.

18. (Currently Amended) A non-volatile or volatile computer-readable medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving an ICMP packet, wherein ~~a data field within~~ the ICMP packet ~~includes~~ carries a portion of a header associated with a connection in a connection-oriented transport protocol, and wherein the portion of the header includes a packet sequence value associated with the connection;

obtaining the packet sequence value from the portion of the header that is ~~included within the data field~~ carried within the ICMP packet;

authenticating the ICMP packet by determining if the packet sequence value from the portion of the header that is ~~included within the data field~~ carried within the ICMP packet is valid; and

responding to the ICMP packet by updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid

19. (Currently Amended) Apparatus for preventing an attack on a network, comprising:

means for receiving an ICMP packet, wherein ~~a data field within~~ the ICMP packet ~~includes~~ carries a portion of a header associated with a connection in a connection-oriented transport protocol, and wherein the portion of the header includes a packet sequence value associated with the connection;

means for obtaining the packet sequence value from the portion of the header that is ~~included within the data field~~ carried within the ICMP packet;

means for authenticating the ICMP packet by determining if the packet sequence value from the portion of the header that is ~~included within the data field~~ carried within the ICMP packet is valid; and

means for responding to the ICMP packet by updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid.

20. (Currently Amended) An apparatus as recited in Claim 19, wherein the means for receiving an ICMP packet comprises means for receiving an ICMP packet , wherein ~~the data field within~~ the ICMP packet ~~includes~~ carries a portion of a TCP header associated with a TCP connection.

21. (Original) An apparatus as recited in Claim 19, wherein the means for receiving an ICMP packet comprises means for receiving an ICMP "endpoint unreachable" error packet.

22. (Original) An apparatus as recited in Claim 19, wherein the means for receiving an ICMP packet comprises means for receiving an ICMP packet that specifies that fragmentation is needed.

23. (Previously Presented) An apparatus as recited in Claim 19, wherein the means for authenticating the ICMP packet by determining if the packet sequence value is valid comprises means for determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection.

24. (Previously Presented) An apparatus as recited in Claim 19, wherein the means for authenticating the ICMP packet by determining if the packet sequence value is valid comprises means for determining if the packet sequence value is within a range of sent but unacknowledged TCP packet sequence values for the connection.

25. (Previously Presented) An apparatus as recited in Claim 19, wherein the means for authenticating the ICMP packet by determining if the packet sequence value is valid comprises means for determining if the packet sequence value is equal to one or more sequence values of one or more packets that are then-currently stored in a TCP re-transmission buffer.

26. (Original) An apparatus as recited in Claim 19, comprising a router acting as a TCP endpoint node.

27. (Original) An apparatus as recited in Claim 19, comprising a firewall device.

28. (Currently Amended) A network element, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to perform the steps of:

receiving an ICMP packet, wherein ~~a data field within~~ the ICMP packet ~~includes~~ carries a portion of a header associated with a connection in a connection-oriented transport protocol, and wherein the portion of the header includes a packet sequence value associated with the connection;

obtaining the packet sequence value from the portion of the header that is ~~included within the data field~~ carried within the ICMP packet;

authenticating the ICMP packet by determining if the packet sequence value from the portion of the header that is ~~included within the data field~~ carried within the ICMP packet is valid; and

responding to the ICMP packet by updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid.

29. (Currently Amended) A network element as recited in Claim 28, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet, wherein ~~the data field within~~ the ICMP packet ~~includes~~ carries a portion of a TCP header associated with a TCP connection.

30. (Previously Presented) A network element as recited in Claim 28, wherein the step of receiving an ICMP packet comprises receiving an ICMP "endpoint unreachable" error packet.

31. (Previously Presented) A network element as recited in Claim 28, wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed.

32. (Previously Presented) A network element as recited in Claim 28, wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection.

33. (Previously Presented) A network element as recited in Claim 28, wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of sent but unacknowledged TCP packet sequence values for the connection.

34. (Previously Presented) A network element as recited in Claim 28, wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is exactly equal to one or more sequence values of one or more packets that are then-currently stored in a TCP re-transmission buffer, starting at a sequence value of a previously sent segment that resulted in receiving the ICMP packet.

35. (Previously Presented) A network element as recited in Claim 28, wherein the steps are performed in a router acting as a TCP endpoint node.

36. (Previously Presented) A network element as recited in Claim 28, wherein the steps are performed in a firewall device.